REMARKS

[0003] Applicant respectfully requests entry of the following remarks and reconsideration of the subject application. The remarks should be entered under 37 C.F.R. §1.116 as they place the application in better form for appeal, or for resolution on the merits.

Request for Withdrawal of Finality

[0004] In accordance with MPEP 706.07(d), Applicant submits that the final rejection is premature. Applicant formally asks that the Examiner reconsider finality on of the rejections in this Action. Applicant submits that the Examiner should withdraw finality because final rejections were based on a reference herein removed under § 103 (c), and Applicant could not have provided evidence of the reference's invalidity earlier since the reference was first cited in the final office action. Applicant further submits that the Examiner should withdraw finality because the Examiner failed to provide specific rejections and reasoning for rejection addressing specific claimed aspects of at least claim 14 .

[0005] Since the rejections of currently presented claims 1-5, 8-13 and 22-27 are incomplete, having been based in part on an invalid reference, Applicant submits that these rejections cannot properly be maintained. Accordingly, Applicant respectfully

requests the Examiner to withdraw the rejections of these claims. Applicant further asserts that these claims are allowable.

[0006] Applicant submits that the Examiner has failed to address specific claim language in at least claim 14. Specifically, regarding claim 14:

- identifying information contained in the security-related event; [and]
- identifying a second security-related application program associated with the information contained in the security-related event;

[0007] It is not that the Examiner disagreed about whether specific claim language distinguishes the claims from the cited references. Rather, it appears that the Examiner ***has not addressed*** whether specific claim language distinguishes the claims from the cited references.

[0008] With few exceptions, the Examiner provides little to no explanation as to how specific components of the cited reference correspond to the actual claim language. Furthermore, the Office provides little or no explanation as to how the operation of components of the cited reference specifically corresponds to that of the actual claim language.

[0009] Since the Examiner has provided little or no reasoning for its rejections, Applicant can do little more than gainsay. Applicant is forced to make assumptions and guesses as to the Examiner's specific reasoning. Therefore, Applicant submits that it has been denied its right to adequately and effectively respond to the Office's rejections.

[0010] In *In re Lee*, 61 USPQ2d 1430 (CA FC 2002), the Federal Circuit explained the following on page 1433:

> The Administrative Procedure Act, which governs the proceedings of administrative agencies [such as the Patent and Trademark Office] and related judicial review, establishes a scheme of "reasoned decisionmaking." Not only must an agency's decreed result be within the scope of its lawful authority, but the process by which it reaches that result must be logical and rational. Allentown Mack Sales and Service, Inc. v. National Labor Relations Bd., 522 U.S. 359, 374 (1998) (citation omitted).
>
> This standard requires that the agency not only have reached a sound decision, but have *articulated the reasons for that decision*. The reviewing court is thus enabled to perform meaningful review within the strictures of the APA, for the court will have a basis on which to determine "whether the decision was based on the relevant factors and whether there has been a clear error of judgment." Citizens to Preserve Overton Park v. Volpe, 401 U.S. 402, 416 (1971). [emphasis added]

[0011] Applicant submits that the Office has generally failed to articulate the reasons for its decision-making. Accordingly, Applicant requests that the Office withdraw finality and completely re-examine all of these claims anew.

CITED ART SUBJECT TO OBLIGATION OF ASSIGNMENT TO SAME ASSIGNEE – 35 U.S.C. § 103 (C)

[0012] The Applicant respectfully requests that the Examiner remove U.S. Patent Application Publication 2003/0236994 as a prior art reference in prosecution of the instant application as a result of the following statement as set forth in the Manual of Patent Examining Procedure, 706.02(l)(2) II,

[0013] The instant application and the cited reference, U.S. Patent Application Publication 2003/0236994, were, at the time the invention of the instant application was made, subject to an obligation of assignment to Microsoft Corporation. Applicant respectfully submits that the cited art, U.S. Patent Application Publication 2003/0236994, only qualifies as prior art under § 102(e), and shared a common assignee with the instant application at the time the subject matter of the instant application was conceived. Thus, U.S. Patent Application Publication 2003/0236994, cited in combination with Willebeek-Lemair, U.S. Patent Application Publication 2003/0204632, under § 103(a) should be disqualified under § 103(c).

[0014] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-5, 8-17, and 19-32 are presently pending. Claims amended herein are none. Claims withdrawn or cancelled herein are 6-7 and 18. New claims added herein are none.

Statement of Substance of Interview

[0015] Examiners Young and LaForgia spoke with me—the undersigned representative for the Applicant—on Aug. 8, 2007. Applicant greatly appreciates the Examiners' willingness to talk. Such willingness is invaluable to all of us in our common goal of an expedited prosecution of this patent application.

[0016] During the interview we discussed §101 issues, proposed claim amendments, and removal of a reference that was newly cited in the Final Rejection.

Formal Request for an Interview

[0017] If Examiner Young's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can resolve any outstanding issues quickly and efficiently by phone.

[0018] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Substantive Matters

Claim Rejections under § 101

[0019] The Examiner rejects claims 22-27 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicant respectfully traverses the rejections of these claims. Applicant submits that these claims comply with the patentability requirements of § 101 and that the § 101 rejections should be withdrawn for the reasons presented below. The Applicant further asserts that these claims are allowable. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Independent Claim 22

[0020] The Examiner indicates (Action, p. 2-3) the following with regard to this claim:

> ***Claim Rejections - 35 USC § 101***
>
> 35 U.S.C. 101 reads as follows:
>
> **Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.**
>
> Claims 22-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
>
> Claim 22 teaches a system comprised of a first security engine, a second security engine and an event manager. The specification defines security engines as "implemented in software, hardware, or a combination of both." It is further stated, that the event manager receives events from the security engines and then "processes these events and communicates the information contained in particular events to other search engines." The Examiner interprets the event manager to recite software.

Therefore, the entire claim recites software, which fails to fall into one of the 4 categories of invention. The dependent claims 23-27 limit the software of independent claim 22, so they are non-statutory as well.

The rejection for claims 22-27 under 35 U.S.C. 101 stands as the amendment filed 2/23/2007 does not recite enough structure. The Examiner suggests modeling claim 22 after statuary claim 28.

[0021] Applicant submits that "*A system implemented at least in part by a computing device*" meets §101 standards. A **device** being inherently tangible. Noting that *tangible* added to claim 28 in amendment in order to expedite prosecution, overcame an earlier §101 rejection of that claim, the tangible device as presented by claim 22 should also be sufficient to overcome the outstanding rejection.

[0022] The Examiner's interpretation that "the event manager . . . recite[s] software. Therefore, the entire claim recites software . . ." is flawed and fails to consider the claim as a whole. When considered as a whole the claim recites more than software since it includes "A system implemented at least in part by a computing device, comprising: a first security engine . . . ; a second security engine . . . ; and an event manager **coupled** to receive events from the first security engine and the second security engine, the event manager further to . . . **communicate the information** contained in the particular event **to the at least one security engine.**"

[0023] The term "coupled" when considered in the context of the entire claim directed to a system implemented by a tangible device further indicates tangibility. Additionally, the claim includes the event manager *communicating* information in a system implemented by a tangible device. It appears that the Examiner read the provision that security engines could be implemented in either software, hardware, or

both as applying to the event manager and then the system in toto, yet the claim recites *a computing device*.

[0024] The indication that the claim "does not recite enough structure," seems to indicate a size or amount threshold that is not present in § 101. Thus, Applicant respectfully requests that these rejections be withdrawn.

Dependent Claims 23-27

[0025] These claims ultimately depend upon independent claim 22. As discussed above, claim 22 recites more than software and is directed to statutory subject matter. Thus, the dependent claims are also directed to statutory subject matter for at least the same reasons. The dependent claims may also be directed to statutory subject matter for additional independent reasons.

Claim Rejections under §§ 102 and 103

[0026] The Examiner rejects claims 14-17, 19-21, and 28-32 under §102. For the reasons set forth below, the Examiner has not shown that cited reference anticipates the rejected claims.

[0027] In addition, the Examiner rejects claims 1-5, 8-13, and 22-27 under §103. For the reasons set forth below, the Examiner has not made a prima facie case showing that the rejected claims are obvious.

[0028] Accordingly, Applicant respectfully requests that the § 102 and/or § 103 rejections be withdrawn. Applicant further asserts that these claims are allowable, and respectfully requests that the case be passed along to issuance.

[0029] The Examiner's rejections are based upon the following references alone and/or in combination:

- **Willebeek-Lemair**: *Willebeek-Lemair, et al.,* U.S. Patent Application Publication 2003/0204632 (published Oct. 30, 2003);
- **Cedar**: *Cedar, et al.,* U.S. Patent Application Publication 2003/0236994 (published Dec. 25, 2003).

[0030] Cedar is herein removed as a reference under 35 U.S.C. § 103(c).

Overview of the Application

[0031] The Application describes a technology for enhancing the security of a computing system by sharing events, such as security-related events, among multiple security engines. In a particular embodiment, an event is received from a first security engine. A second security engine is identified that can utilize information contained in the event. The information contained in the event is then communicated to the second security engine.

Cited References

[0032] The Examiner cited Willebeek-Lemair as the primary reference in anticipation- and/or obviousness-based rejections. The Examiner cited Cedar, herein removed as a reference under 35 U.S.C. § 103(c), as the secondary reference in obviousness-based rejections.

Willebeek-Lemair

[0033] Willebeek-Lemair describes a technology for network discovery functionality, intrusion detector functionality and firewalling functionality integrated together to form a network security system presenting a self-deploying and self-hardening security defense for a network.

Anticipation Rejections

[0034] Applicant submits that the anticipation rejections are not valid at least because, for each rejected claim, no single reference discloses each and every element of that rejected claim.[1] Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.[2]

Based upon Willebeek-Lemair

[0035] The Examiner rejects claims 14-17, 19-21, and 28-32 under 35 U.S.C. § 102(e) as being anticipated by Willebeek-Lemair. Applicant respectfully traverses the rejections of these claims. Based at least on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

Independent Claims 14 and 28

[0036] The Examiner indicates the following with regard to claim 14 (Action, p. 3-4) and claim 28 (Action, p. 5-6) :

> **Claim 14:**
>
> Paragraph [0014] teaches an intrusion detector functionality that sends an alert when detecting potentially harmful traffic. This is sent to a firewall, which responds by blocking the entrance of the detected traffic. The Examiner interprets the intrusion

[1] "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); also see MPEP §2131.

[2] See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

detector and firewall to be "security engines" of claim 1. This would then teach one security engine (intrusion detector) detecting an event (potentially harmful traffic), identifying a second security engine (firewall), and communicating the event to it. Paragraph [0075] teaches that the network discovery functionality maintains a database that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

Claim 28:

Figure 2 shows a network defense system that includes a security management agent and two security engines (an intrusion detector functionality and a firewalling functionality). As shown the security management agent has the functionality to receive alerts from one of the security engines listed and communicate the alert to the other. Paragraph 81 explains the implementation of system 10 in Figure 2. It teaches a threat prevention appliance 500 that utilizes system 10 and is "configured as a network element in the protected network 14." The Examiner interprets this functionality as a computer program and the network element as a computer-readable medium. Paragraph [0075] teaches that the network discovery functionality maintains a database that also includes "host/service inventory information which includes an inventory of assessed vulnerabilities." The Examiner interprets this to include system state information.

[0037] Applicant submits that Willebeek-Lemair does not anticipate these claims at least because it does not show or disclose the following from claim 14 (equally applicable to claim 28) "receiving a security-related event from a first security-related application program, the security related event being associated with a system state."

[0038] In this Action, the Examiner apparently equates the claimed "security-related application programs" with the security engines of claim 1 and then those with the intrusion detector and firewall disclosed by Willebeek-Lemair. Additionally, the Examiner *interprets* and equates host/service inventory information maintained in a database by network discovery functionality disclosed by Willebeek-Lemair as the "security related event being associated with a system state" recited in this claim. Applicant respectfully disagrees.

[0039] Unlike the "security related event being associated with a system state" of the claim, the information of Willebeek-Lemair is not characterized as including "information regarding the current operating state or operating mode of host computer . . . [or] how host computer . . . is configured." The information of Willebeek-Lemair is defined as stored data that "may comprise, for example, host/service inventory information which includes an inventory of assessed vulnerabilities of the network." The "host/service inventory information" of Willebeek-Lemair is directed to network vulnerabilities and does not include "System state information [that] includes information regarding the current operating state or operating mode of host computer . . . [or] how host computer . . . is configured." To support this assertion, Applicant refers to the paragraph [0075] of Willebeek-Lemair and the definition of system state information provided in the Specification at least at (p. 5, ll. 17-21).

[0040] Furthermore, the rejections do not address the all of the remaining steps of the claims.

Dependent Claims 15-17, 19-21, and 29-32

[0041] These claims ultimately depend upon independent claims 14 or 28. As discussed above, claims 14 and 28 are allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0042] Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a prima facie case have not been met.

Claims rejected based on removed reference

[0043] Claims 1-5, 8-13, and 22-27 were rejected based on U.S. Patent Application Publication 2003/0236994, to Cedar et al., cited in combination with Willebeek-Lemair under § 103(a). Cedar is herein removed as a reference under § 103(c). All of the claimed elements and features of these claims are not disclosed by the remaining reference. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of these claims. Applicant further asserts that these claims are allowable.

Dependent Claims

[0044] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0045] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call/email me or my assistant at your convenience.

Respectfully Submitted,

Dated: 08/16/2007

By: 

Bea Koempel-Thomas
Reg. No. 58,213
(509) 324-9256 x259
bea@leehayes.com
www.leehayes.com

My Assistant: Carly Bokarica
(509) 324-9256 x264
carly@leehayes.com